

# Encrypted Client Hello Deployment Considerations

Andrew Campling [Andrew.Campling@419.Consulting](mailto:Andrew.Campling@419.Consulting)

Arnaud Taddei [Arnaud.Taddei@broadcom.com](mailto:Arnaud.Taddei@broadcom.com)

Simon Edwards [Simon.Edwards@broadcom.com](mailto:Simon.Edwards@broadcom.com)

Paul Vixie [Paul@Redbarn.Org](mailto:Paul@Redbarn.Org)

David Wright [David.Wright@SWGfL.Org.UK](mailto:David.Wright@SWGfL.Org.UK)

# Context

- Encrypted Client Hello (ECH) is “a mechanism in Transport Layer Security (TLS) for encrypting a ClientHello message under a server public key”
- Builds on the previous Encrypted Server Name Indication (eSNI) proposal
- Being developed within the IETF’s TLS working group
- See <https://datatracker.ietf.org/doc/draft-ietf-tls-esni/> for the latest version (currently draft -16)

# What is the Issue?

- RFC 8744 – “Issues and Requirements for Server Name Identification (SNI) Encryption in TLS”
  - Includes a brief description of what it characterises as "unanticipated" usage of SNI information (section 2.1)
  - A brief assessment of alternative options in the event that the SNI data is encrypted (section 2.3)
  - Asserts that "most of [the unanticipated usage] functions can, however, be realized by other means“
- The data encapsulated by ECH is of legitimate interest to on-path security actors including anti-virus software, parental controls [and other content filtering] and consumer and enterprise firewalls – there’s a lot of running code!
- Some end user groups (eg Fortune 500 CISOs) are becoming very concerned about the implications for their cybersecurity, organisational policy on content access etc

# Supporting End Users

The current ECH Deployment Considerations draft includes:

- Observations on current use cases for SNI data in a variety of contexts, clarifying why it is preferred to DNS
- Reasons why the use of that data is important to the operators of both public and private networks (eg enterprises and educational establishments)
- Information on how the loss of access to SNI data will cause difficulties in the provision of services to end-users, complicates support for BYOD and potentially weakens cybersecurity

In addition, some mitigations are identified that may be useful for inclusion by those considering the adoption of support for ECH in their software.

# If ECH Deployment Considerations Interests You....

- The current version of the draft is at:
  - <https://datatracker.ietf.org/doc/draft-campling-ech-deployment-considerations/>
  - To be updated with an -07 version shortly
- To engage on this topic:
  - Speak to Arnaud Taddei ([Arnaud.Taddei@broadcom.com](mailto:Arnaud.Taddei@broadcom.com)) or Andrew Campling ([Andrew.Campling@419.Consulting](mailto:Andrew.Campling@419.Consulting)) – both here all week
  - Use the public GitHub page at <https://github.com/echdeploy/draft-ech-deployment-considerations>

If you want to work on the design of ECH itself, go to the TLS working group

Thank You